Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

~ Gmail To Issue Warning! ~ People Are Talking! ~ "Fallout 4" Review!
~ JP Morgan Hacking Bust! ~ Attack the Hyperlink? ~ Updates to Chrome?
~ Apple Certificates Goof ~ Facebook Blocking Tsu! ~ NSA Disclosures, Huh?

~ Windows 10 Major Update ~ Chrome Support Update! ~ Chrome Patch Pulled!

-* The Rise of the Tomb Raider! *-
-* Microsoft Tries To Evade US Spying! *-
-* Belgium to Facebook: Stop Tracking Them! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

If you've been following today's international news, you're aware of the terrorist attacks that occurred in Paris this evening. It's been difficult keeping my eyes off of the television trying to keep updated. If I heard correctly, the terrorists have been caught (and/or taken out) and continued investigations are ongoing. With all that has been occurring in the world recently (the Russian plane beeing blown up, attacks in Lebanon, the attacks on ISIS, etc.) one has to wonder about possible retaliations.

Our thoughts and prayers go out to the people of France, especially to the victims and their families.

Until next time...

=~=~=~=

->In This Week's Gaming Section - Fallout 4: A Fanboy s Op-ed Review!
""""""""""""""""""""""""""""""""" The De-Objectification Of Lara Croft Is Complete!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

Fallout 4: A Fanboy s Op-ed Review

When I finished Fallout 3, the game left me with one desire: please let there be another installment soon.

Fallout New Vegas tried to fill the need, but opinions among Fallout fans were split. Some loved "West Coast Fallout," replete with motorcycle gangs, delusional wannabe Romans, and one super-depressed kid named Boxcars. Others hoped for something more evolutionary, something that didn't just add to the Fallout universe but deeply improved upon it. For that sort of game, fans had to wait for Fallout 4. So we waited... for more than half a decade. And the wait was indeed worth it.

We've already run our review of the new game, but I wanted to offer a slightly different perspective: how Fallout 4 feels to someone who is deeply invested in the Fallout universe. That is, how it feels to a Fallout fanboy which I'm proud to be. As such, I will look at the game only as it relates to Fallout 3 and to New Vegas, with no regard for how it stacks up to other titles in the RPG genre.

Bottom line: if you did not like Fallout 3, you are not going to like Fallout 4. The two games are built around the Fallout pillars of random wasteland events, wild side quests, challenging character development, and imagining the post-nuclear apocalyptic world. But if you're a Fallout series fan, it's time to clear some serious space on your calendar.

A winner

Fallout 4 looks and plays significantly better than Fallout 3, which is not a knock on Fallout 3 (now seven years old). Playing on the Xbox One, I tested Fallout 4 on both a 48-inch HD Samsung TV (five years old) and a 78-inch 4K Samsung TV (brand new).

Performance is better than Fallout 3 was at its release, but Fallout 4 is not without its glitches, particularly in the clipping department. I was saved from being totally annihilated by a Sentry Bot simply because it got stuck on a rock and I ran away. Once I got stuck in a pile of car parts while in Power Armor. I couldn't get out. Autosave to the rescue.

The overall environment looks terrific. Downtown Boston is more colorful than the Capitol Wasteland, and its outskirts have more foliage. The environment exhibits changing weather, from storms to fallout to fog. The visual glitches that pop up don't bother me much, in part because I expect they will be fixed quickly. As for what won't be changed, yes, some of the scenery is bland and some of it is repetitive. But I think that's an acceptable trade-off. I can't think of any game this packed with content that doesn't reuse textures, buildings, etc. to some degree, and I'd rather have 100+ hours of repeatable gameplay than have a world constrained by new art.

The world of Fallout 4 is massive compared to Fallout 3, and Fallout 3 was breathtaking in its expanse. I've read the reviews that say that the new graphics are unacceptable, but I can't agree. The graphics could be better, sure, but nothing about the game's visual design has diminished my enjoyment.

...no, really. You can find retro-themed games to load on Pip-Boy throughout Fallout 4.

As for the story, I think it's great. It didn't take me long to get invested in my character and my quests probably two hours. I

certainly did find it difficult to stay on one course because I was constantly running off one direction or another to check out a weird playground, an abandoned house, a cave, a really loud explosion, or whatever other strange phenomenon the game would throw my way. But the overwhelming variety of subquests and distractions is simply part of the series' appeal.

As the game evolves, you will meet different factions, and those factions are frankly a little more interesting than those from Fallout 3 (with the exception perhaps of the vampires, which were awesome). The factions also load you up with things to do, so there's rarely a dull moment that Fast Travel can't solve by taking you someplace else.

There are a few enhancements worth noting. In Fallout, you are essentially a scavenger. You open lockers, boxes, and the pockets of dead people. In the past, searching would open a transfer UI, you'd select what you wanted and then hit "exit" (B on the Xbox) to back out. At minimum, you had two button presses to look and then exit, and then another set of presses if you wanted to take anything. In Fallout 4, you merely point your reticule over a dead body or a file cabinet and the UI reveals its contents. You can take it all quickly (push X) and move on, or you can pick through it (push A). This is a huge time saver, effectively eliminating two button presses on everything you look into. In Fallout, that should be nearly everything.

While the first-person action is better this time around, my scav-minded self was mostly in ammo conservation mode, preferring to use V.A.T.S. Thankfully, V.A.T.S. no longer stops time. Instead, you enter slow-motion, something akin to "Bullet Time." This removes a real crutch (stopping time to shoot), while at the same time making V.A.T.S. more enjoyable to use. You can watch a shot develop (watch as the raider foolishly lifts his head), or you can watch a pack of feral ghouls bear down on you even in slow motion, thereby increasing the panic of the ghoul rush.

Where V.A.T.S. might have saved you in the past by giving you a ton of time to calculate your move, now it might not be enough. (It's worth noting that popping up your PipBoy does still stop time, but now boosters like eating, using stimpacks, etc., do not take instant effect. Their application will come after you exit the PipBoy.)

Another quick point about V.A.T.S.: luck is now useful to cultivate, as you can choose when to apply a critical hit while in V.A.T.S. It's a nice touch that can save your hide.

The D-Pad also sports a deeper favorite items system, allowing you to store multiple items in each direction. I found this extremely useful, using "Right" for handguns, "Left" for rifles (with the sniper rifle far left), and "Up" for close-quarter weapons. I then stashed my aids in the "Down" menu and found that I simply didn't need to get into the Pip-Boy as often. These tweaks make the game that much more viable as a first-person shooter.

The new SPECIAL system is also an improvement. Our official review saw it as confusing and unnecessarily complex, but I actually feel that it is simplified from previous incarnations.

While you do have fewer points to spend at each level (one instead of two, usually), I think this ultimately adds up to a better experience. In Fallout 3, it was often the case that you would just pick the best perks from the small handful that had been unlocked. You had to wait for level increases and other boosts before other perks were even available to ponder. This new system provides a lot more flexibility in character development, allowing you to see all of the options and the effects, even letting you to put extra points into the perks. When I first played Fallout 3, I remember being confused about how I should develop my character. Now I can look at the new, illuminating visual presentation of SPECIAL and perks and easily chart where I want to go next.

Then there’s the soundtrack, something that’s sacred to most Fallout fans. The soundtrack has gone in a direction that I really appreciate. While New Vegas took the soundtrack to a very Western/country/cowboy theme, with Fallout 4 we are back in a world filled with GNN, Billy Holiday, Danny Kane, and most of the classics from Fallout 3. There are plenty of new songs, too, but there’s just something amazing about being in an irradiated cave jamming, "Bongo, bongo, bongo, I don’t wanna leave the Congo..." Some of the songs created just for Fallout 4 are fairly humorous.

Also humorous is the hilarious stuff raiders talking about when chatting with one another: substance abuse, significant others, fear of fire, and so on. The game is again replete with great writing, particularly when you’re checking out the logs on various terminal screens. Holotape audio recordings are more interesting now, too.

The game isn’t without issues. Much has been written online, including here at Ars, about poor facial animations and the like. These have never been a strong point of any Fallout title, and they are certainly a weaker point of this game. That said, it feels to me more like a minor issue than anything fans of the series will find off-putting.

Here’s my take: if you are a fan of the Fallout series, particularly in its modern incarnations, you are going to be a fan of this game. The graphics are better, the user interface is smartly improved, combat feels tighter, crafting is both easier and more meaningful, and the quota of wacky, crazy side quests and events has definitely been increased.

This is the kind of game that you live with, that you make a part of your life for a very long time. It’s a game in which you are totally free to jump between quests, to go off on bizarre expeditions that at first seem meaningless, or to spend some time just tightening up your settlement. In the week I’ve had my copy, it keeps calling to me, and I keep playing Fallout 4 over a host of other new games I have sitting around. And I suspect that isn’t going to change for a while.

With ’Rise of the Tomb Raider,’ The De-Objectification Of Lara Croft Is Complete

You might not know this, but a really good video game came out today. No, not Fallout 4, which is currently drowning the world in hype and stellar review scores, but Rise of the Tomb Raider, the timed Xbox exclusive from Square Enix/Crystal Dynamics that marks a return to the recently rebooted series with a younger, fresher Lara Croft.

While I understand that holiday season is a crowded time and last week was Black Ops 3 and next week is Battlefront, I still think Tomb Raider could have found a better date so it didn t get totally drowned out. But with those good reviews, hopefully people will pick it up all the same.

I ll save thoughts on gameplay for another time, but I really was struck by how with Rise of the Tomb Raider, Lara Croft has now fully transformed from the comically proportioned sexpot of the video game world to possible one of its most progressive, feminist icons. In this new game, Crystal Dynamics have effectively done away with objectifying Lara Croft at all.

There was progress made in the last game, the original reboot that had a teenaged Lara wearing pants and let her keep her athletic build, but shrunk her chest down a few cup sizes from past installments. And yet, most of the game did have her soaking wet in a tank top, and put her in situations where the camera seemed trained on her rear end. The game also had an almost weird obsession with seeing Croft die in horribly graphic ways after failing gameplay segments or quicktime events. That wasn t explicitly sexual, but it was a bit creepy all the same.

In Rise of the Tomb Raider, pretty much all remnants of the past objectification of Lara have been banished. Out of about ten different outfits I unlocked for Croft over the course of the game, only one was her classic tank top (which manages to be less revealing than ever), and the vast majority of choices were bulky jackets that were more than weather appropriate given that the game mostly takes place in Siberia. And the outfits that actually gave you bonus perks like faster health regen were ones that put Lara in full military camo like Solid Snake. While a completionist reward outfit for someone like Croft in other games probably would have been a bikini, when you clear all the game s tombs to unlock one final ensemble, you re given what s essentially a full suit of medieval plate armor.

Gone are the butt-focused camera shots, and there are only a couple of graphic deaths as opposed to the dozens that were present in the last game. Though the game also features male characters, Croft isn t forced into a love story, focusing on the mission at hand of, you know, not dying. Nor is she ever made a damsel, as at different points in the game she rescues each of the two main guys in the story.

It s not that Lara Croft is no longer attractive. She still is, at least by CG-animated beauty standards. But her appearance is not relevant to the narrative, nor is it spotlighted as eye-candy for the player. Lara Croft used to be the literal pin-up girl for video game vixens, but now she s just a badass, not meant to titillate in the least.

Has the series lost anything because of this transformation? No,

and Tomb Raider is now actually better than it s ever been, both in terms of narrative and gameplay. It s not without its lingering issues, but whatever the problems are, they have nothing to do with whether or not Croft is sexualized for the player.

I m definitely not in the no woman should show skin or have sex appeal camp of game design, but I do recognize that more often than not, when modern games are trying to make sexy characters the way they used to in years past, it just falls flat. I m thinking of Quiet from Metal Gear Solid 5, a pretty great character completely ruined by Hideo Kojima s junior high-level interest in boobs. Then in contrast, here we have Lara Croft who went from the most objectified woman in gaming to now one of the least. That s a pretty significant development.

I m not saying there should never be a situation where Croft is allowed to act seductively or dress provocatively if it s relevant to the story (charming an antiques dealer at a black tie party, maybe? Just spit-balling). But if her story is about raiding tombs in Siberia and defending an ancient treasure from evil mercenaries, sex and sex appeal really does not factor into that.

In this sense, Rise of the Tomb Raider is a pretty significant achievement for Lara Croft as a character, and gaming at large. Obviously representation of women in games still has a long way to go, but with games like this, it does feel like it s getting better.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

NSA Discloses 91% of Bugs It Finds But Doesn’t Say When It Discloses Them

With one answer from the NSA comes a myriad of questions.

In an effort to increase transparency, the U.S. National Security Agency (NSA) revealed in a press release last month it discloses 91% of vulnerabilities it finds in software made and/or used in the U.S. to developers. But the NSA doesn’t say what it does before it discloses those vulnerabilities, or when it discloses them.

The NSA’s press release notes that the remaining 9% of vulnerabilities are either spotted and patched by the developers before the NSA discloses, or are "not disclosed for national security reasons."

The NSA says that disclosure means it forgoes the opportunity to gather foreign intelligence, prevent theft of U.S. intellectual property and find more security bugs, but that its "bias" is to disclose regardless.

However, the NSA is careful to not say when it discloses, or what it does before it discloses security flaws.

However, the NSA is careful to not say when it discloses, or what it does before it discloses security flaws.

Based on information from current and former U.S. government officals, Reuters reports that the NSA only discloses bugs after it creates its own vulnerability-exploiting attacks.

In the documents Edward Snowden leaked in 2013, it was revealed that the NSA spent $25 million in 2013 to buy "zero-day" software vulnerabilities from "private malware vendors." Zero-days are software flaws that have yet to be disclosed to the public or the companies that developed the software, opening up the potential for exploitation. The name refers to the severity of the vulnerability, meaning that if a company was made aware of a zero-day, it would need to disclose and issue a fix immediately.

Reuters reported in 2013 that the U.S. government was the largest buyer of zero-day vulnerabilities.

Speaking to Reuters, a former White House official said that it’s "reasonable" to assume the NSA exploited most of vulnerabilities it found before disclosing them to their respective developers. Additionally, the official said that the 91% of disclosures likely includes vulnerabilities it bought.

In a post-Snowden world, the NSA is under increased scrutiny about the data it collects and the means by which it collects it, hence press releases are designed to paint the organization in a good light. In being vague, this particular press release has raised more questions.

Microsoft To Host Data in Germany To Evade US Spying

Microsoft’s new plan to keep the US government’s hands off its customers’ data: Germany will be a safe harbor in the digital privacy storm.

Microsoft on Wednesday announced that beginning in the second half of 2016, it will give foreign customers the option of keeping data in new European facilities that, at least in theory, should shield customers from US government surveillance.

It will cost more, according to the Financial Times, though pricing details weren’t forthcoming.

Microsoft Cloud - including Azure, Office 365 and Dynamics CRM Online - will be hosted from new datacenters in the German regions of Magdeburg and Frankfurt am Main.

Access to data will be controlled by what the company called a German data trustee: T-Systems, a subsidiary of the independent German company Deutsche Telekom.

Without the permission of Deutsche Telekom or customers, Microsoft won't be able to get its hands on the data. If it does get permission, the trustee will still control and oversee Microsoft's access.

Microsoft CEO Satya Nadella dropped the word "trust" into the company's statement:

> Microsoft s mission is to empower every person and every individual on the planet to achieve more. Our new datacenter regions in Germany, operated in partnership with Deutsche Telekom, will not only spur local innovation and growth, but offer customers choice and trust in how their data is handled and where it is stored.

On Tuesday, at the Future Decoded conference in London, Nadella also announced that Microsoft would, for the first time, be opening two UK datacenters next year. The company's also expanding its existing operations in Ireland and the Netherlands.

Officially, none of this has anything to do with the long-drawn-out squabbling over the transatlantic Safe Harbor agreement, which the EU's highest court struck down last month, calling the agreement "invalid" because it didn't protect data from US surveillance.

No, Nadella said, the new datacenters and expansions are all about giving local businesses and organizations "transformative technology they need to seize new global growth."

But as Diginomica reports, Microsoft EVP of Cloud and Enterprise Scott Guthrie followed up his boss s comments by saying that yes, the driver behind the new datacenters is to let customers keep data close:

> We can guarantee customers that their data will always stay in the UK. Being able to very concretely tell that story is something that I think will accelerate cloud adoption further in the UK.

Microsoft and T-Systems' lawyers may well think that storing customer data in a German trustee data center will protect it from the reach of US law, but for all we know, that could be wishful thinking.

Forrester cloud computing analyst Paul Miller:

> To be sure, we must wait for the first legal challenge. And the appeal. And the counter-appeal.
>
> As with all new legal approaches, we don t know it is watertight until it is challenged in court. Microsoft and T-Systems lawyers are very good and say it's watertight. But we can be sure opposition lawyers will look for all the holes.

By keeping data offshore - particularly in Germany, which has

strong data privacy laws - Microsoft could avoid the situation it's now facing with the US demanding access to customer emails stored on a Microsoft server in Dublin.

The US has argued that Microsoft, as a US company, comes under US jurisdiction, regardless of where it keeps its data.

Running away to Germany isn't a groundbreaking move; other US cloud services providers have already pledged expansion of their EU presences, including Amazon's plan to open a UK datacenter in late 2016 that will offer what CTO Werner Vogels calls "strong data sovereignty to local users."

Other big data operators that have followed suit: Salesforce, which has already opened datacenters in the UK and Germany and plans to open one in France next year, as well as new EU operations pledged for the new year by NetSuite and Box.

Can Germany keep the US out of its datacenters? Can Ireland?

Time, and court cases, will tell.

Belgium to Facebook: Stop Tracking Non-Facebook Users or Face $267K Daily Fines

Max Schrems must be pleased.

He who rose up from the ranks of Facebook's privacy-ravaged users to file complaints against what he said was Facebook's illegal data collection/retention is now witnessing the fruits of his labor.

Or, as he tweeted in response to the Belgian court giving Facebook 48 hours to stop tracking those without Facebook accounts, lest it face substantial penalties, "*WOW*":

> Max Schrems @maxschrems
> *WOW* @SophieKwasny: episode Belgium v. Facebook. Judge gives 48 hours to conform to law or will be fined 250000 euros / day

As the AFP reports, Belgium set the clock ticking on Monday, saying that Facebook would face fines of up to 250,000 EUR ($267,000 USD) a day if it doesn't comply within 48 hours.

Facebook said it will appeal.

The AFP quotes the court decision:

> Today the judge... ordered the social network Facebook to stop tracking and registering internet usage by people who surf the internet in Belgium, in the 48 hours which follow this statement.
>
> If Facebook ignores this order it must pay a fine of 250,000 euros a day to the Belgian Privacy Commission.

The court order is the latest salvo in the Europe v. Facebook privacy battle.

It follows a case lodged by Belgium's privacy watchdog - the Belgian Privacy Commission (BPC) - which dragged Facebook into court in June for allegedly "trampling" over Belgian and European privacy law.

In June, the court said that Facebook indiscriminately tracks internet users - even non-Facebook users - when they visit its pages or pages on other sites with "like" or "share" buttons.

Since then, the BPC's lawyers have called Facebook "as bad as the NSA [National Security Agency]."

This 48 hours or-else decision is only the latest EU action against private data flowing into Facebook.

Last month, the EU's highest court struck down the transatlantic Safe Harbor agreement, which had allowed companies to transfer European citizens' personal data to the US, calling the agreement "invalid" because it didn't protect data from US surveillance.

At the heart of the recent Belgian court case is a move Facebook made in June 2014 to give advertisers more ammunition to target users, by mixing data about what we do on its site with data about what we do on other sites.

The Belgian court on Monday said that Facebook does indeed use a special cookie that visitors pick up if they visit a friend's page on Facebook or any other page on the web with Facebook like or share code in it - all without the visitor having ever signed up for a Facebook account.

That cookie stays on a given device for up to two years, enabling Facebook to keep track of people and what they've looked at on the web.

AFP quotes the court's statement:

> The judge ruled that this is personal data, which Facebook can only use if the internet user expressly gives their consent, as Belgian privacy law dictates.

Facebook calls that cookie the "datr" cookie and says it's safe.

Safe, or maybe even some type of prophylactic infosec wonder cookie.

In the recent "Facebook is as bad as the NSA" rhetoric swap, Facebook claimed that its cookies keep Belgium from becoming "a cradle for cyber terrorism."

AFP quotes a statement from Facebook about its appeal of Monday's court decision:

> We've used the datr cookie for more than five years to keep Facebook secure for 1.5 billion people around the world.
>
> We will appeal this decision and are working to minimize any disruption to people's access to Facebook in Belgium.

Meanwhile, back on its home turf, Facebook is having a much easier time of it with a US regulator - the Federal Communications Commission (FCC) - having recently shrugged off the notion that it should trouble Google or Facebook with demands to honor "Do not track" requests.

The FCC dismissed a petition from rights group Consumer Watchdog, which had called on the commission to require "edge providers" - a catch-all term covering websites and apps, including Google, Facebook, YouTube, Pandora, Netflix, and LinkedIn - to honor such requests from consumers.

The FCC's rationale: it doesn't have the authority.

Consumer Watchdog thinks otherwise, and it's reportedly considering an appeal.

Three Indicted for Massive Hack and Fraud Scheme That Targeted JPMorgan

US federal prosecutors, on Tuesday, unveiled criminal charges against three men accused of orchestrating the biggest theft of customer data from financial institutions in the country's history - encompassing personal data belonging to more than 100 million people.

Unsealing a 23-count indictment in Manhattan, the Justice Department charged Gery Shalon, Joshua Samuel Aaron and Ziv Orenstein with computer hacking crimes against JPMorgan, as well as other financial institutions, brokerage firms and financial news reporters, including The Wall Street Journal. The trio stand accused of stealing as many as 83 million customer records.

Speaking at a press conference, US Attorney Preet Bharara said:

> The charged crimes showcase a brave new world of hacking for profit. It is no longer hacking merely for a quick payout, but hacking to support a diversified criminal conglomerate.
>
> This was hacking as a business model. The alleged conduct also signals the next frontier in securities fraud sophisticated hacking to steal nonpublic information, something the defendants discussed for the next stage of their sprawling enterprise.

The news finally puts to bed long-standing rumours of Russian shenanigans, instead painting a picture of good, old-fashioned greed. The scam centred around the tried and tested pump-and-dump stock scam that's still very much alive and kicking, as we learned on Monday, when Lisa told us about James Alan Craig who had been using Twitter to manipulate stock prices.

This case is unusual though - pump-and-dumpers usually just spread misinformation in order to drive stock prices in which ever direction serves their needs; they don't hack their way into systems to steal business data.

That’s exactly what happened in this case though and the reasons for it are simple. Not only were the alleged hackers able to glean more intel on the companies they were targeting, which would have given them additional insight into future stock values, they were also able to pick up personal information on specific individuals - a useful tactic in tailoring attacks against them.

And both avenues proved to be extremely lucrative for them, as prosecutors claim they made upwards of $100m through hacking 7 large banks, running their own illegal Bitcoin trading operation and from an online casino.

In fact, according to law enforcement, the operation was so successful that it employed hundreds of people across 75 shell companies created in a number of countries via fake passports.

Prosecutors claim Shalon was the mastermind of the whole operation, saying he was the owner of US-based Bitcoin exchange Coin.mx which he operated with fellow Israeli, Orenstein.

With the help of Aaron, an American, the group allegedly bought up the type of penny stocks so often used in pump-and-dump scams. They then blasted out emails to dupe the unwary into jumping on a bandwagon so full of hype that they reportedly walked out of one deal alone with $2m.

It’s here that the information stolen from JPMorgan, Dow Jones, Scottrade and others came in useful - client and subscriber lists offered up a long line of potential marks.

As for how the trio allegedly broke into JPMorgan and other banks, the indictment says very little. However, it did reference a mutual fund in Boston whose tardiness left the doors to its network wide open in April 2014, when it failed to install a patch for the Heartbleed bug in good time.

According to Attorney Bharara, the sophisticated nature of the scheme was such that many companies could yet be unaware that they have also been targeted:

> Even the most sophisticated companies like those victimized by the hacks in this case have to appreciate the limits of their ability to uncover the full scope of any cyber-intrusion and to stop the perpetrators before they strike again.
>
> If they have been hacked, most likely others have been as well, and even more will be. The best bet to identify, stop and punish cybercriminals is to work closely, and early, with law enforcement. That happened here, and today’s charges are proof of that.

JPMorgan - which confirmed it was "Victim 1" in the superseding indictment - agreed that strong cooperation with law enforcement had been essential "in bringing the criminals to justice" with Scottrade, which had 4.6 million client accounts compromised, and Dow Jones both nodding in mutual agreement.

Shalon and Orenstein were arrested by Israeli Police in July 2015 on an indictment that charged the underlying securities fraud, and both remain in custody in Israel as prosecutors continue to

negotiate their extradition to the US.

Aaron, meanwhile, remains at large, with prosecutors declining to confirm or deny whether they know where he is currently hiding.

Gmail Will Now Warn You Of Unencrypted Incoming Emails

Google has announced that Gmail will soon offer users a warning when they receive messages that were not sent over encrypted connections. The news comes as there is a big push for encryption in emails.

Internet security is becoming increasingly important, and to help warn users if they’re not using encrypted connections, Google has announced that it will introduce a feature in Gmail warning if an email has arrived over a connection that wasn’t encrypted.

Gmail itself already uses HTTPS encryption as a default for connections between browsers and servers, but for a long time the standard for emails was to leave them unencrypted. This made emails easy to intercept.

"Many email providers don’t encrypt messages while they’re in transit. When you send or receive emails with one of these providers, these messages are as open to snoopers as a postcard in the mail," said Google in a blog post.

Despite this, over the last few years Google and other email providers are beginning to change this, as more than 62 percent of emails sent to Gmail addresses by other users are now being encrypted. Emails sent from a Gmail address to another Gmail address are always encrypted, and emails sent from Gmail to other providers are encrypted 82 percent of the time.

Unencrypted messages are a problem because they make for a great target for hackers. In a joint project between Google, the Univeristy of Michigan and the University of Illinois that studied how email security has evolved since 2013, it was found that 94 percent of messages sent to Gmail can now be authenticated, making it much harder for phishers to intercept messages. Despite this, researchers also found that there are "regions of the Internet actively preventing message encryption by tampering with requests to initiate SSL connections."

Given the fact that there are still plenty of email providers that do not encrypt emails by default, it’s likely that most users will begin to see the warnings within the next few months. It’s important to note that most providers, however, do encrypt messages, including Yahoo, Microsoft, and so on.

Facebook Is Blocking an Upstart Rival But It s Complicated

Tsu is a new social network that promises to pay its users for posting content to its site. But if want to share your Tsu profile

with your Facebook friends, too bad. Facebook is blocking all mentions of Tsu.co, the company s web address. You can t share a post to a Facebook feed, leave an Instagram comment or send a Facebook Messenger message containing the URL. Tsu s CEO claims Facebook went so far as to retroactively remove any mention of the site from its archives.

You can t even share news stories about Tsu, something Xeni Jardin, who wrote about the situation for Boing Boing, discovered Friday when she couldn t share the story to her own Facebook feed. On Monday, Tech News Today, covered Facebook s ban on all things Tsu.co, and just like the Boing Boing story, readers soon found themselves unable to share it on Facebook.

On first glance it looks like a conspiracy to keep an upstart social network down. But the situation is far more complicated.

Tsu promises to pay users a percentage of its advertising revenue. But it doesn t base those payouts merely on the number of times someone views your content. It also offers you a cut of the revenue generated by content posted by people you refer to the site. CEO Sebastian Sobczak says the idea is to pay users for the content they post and reward them for helping build the network.

But this model also means users are incentivized to share links to the site not just to increase page views, but to attract new users. That sounds a lot like multi-level marketing, and it s not hard to imagine people taking advantage of the system. It s not surprising then that Facebook might flag the site for spam, especially if the number of people posting spam far outnumbered the legitimate posts.

As of Tuesday evening we still couldn t share the Boing Boing and Tech News Today stories on Facebook without getting an error, but several other stories about Facebook blocking links to Tsu were allowed, so it s clear that Facebook isn t blocking all news coverage of the site. As of Wednesday morning, it s possible to share the two stories on Facebook again.1

Facebook is within its rights to prevent spam, but its scorched-earth policy of retroactively removing posts seems overkill. Either way, the company s decision underscores the power Facebook, which is for many people synonymous with the Internet, has over what users can or can t see. Run afoul of Facebook s spam algorithms, even accidentally, and you can be practically disappeared from the web.

For its part, Facebook says it blocked Tsu because it violated the company s policies. We require all websites and apps that integrate with Facebook to follow our Platform Policy, Facebook spokeswoman Melanie Ensign told WIRED. We do not allow developers to incentivize content sharing on our platform because it encourages spammy sharing and creates a bad experience for people on Facebook.

She said she wasn t aware of errors when sharing Boing Boing and Tech News Daily stories, but said someone probably flagged those links as spam separately from Tsu and the engineering team will look into it.

Facebook, however, has offered to unblock Tsu if the company disables the ability to automatically share posts from Tsu to Facebook. Our automated systems flagged your app for producing spam on our Platform, a Facebook engineer wrote in an email to Tsu, which provided it to WIRED. Our investigation found your app is incentivizing people to share content to both tsu and Facebook concurrently.

'We would just like to be treated equally and fairly.' Sebastian Sobczak, Tsu CEO

In order to come into compliance with this policy, we ask that you remove your app s ability to share to Facebook, the email read. Let us know when you remove this functionality and we will lift the restriction.

Sobczak says the company has no plans to remove the app s ability to post to Facebook. We would just like to be treated equally and fairly, he says. We maintain we do not violate any of their terms and conditions.

Sobczak argues that the analytics dashboard Facebook offers to developers suggested that Tsu had a lower-than-average spam rate compared to other apps. He also doesn t understand why getting flagged for spam would prompt the removal of old posts containing links to Tsu. And he argues that Tsu doesn t actively incentivize users to post to Facebook, because Tsu users are paid only if someone visits their Tsu page. They aren t paid simply for posting content to Facebook. In that sense, he argues, the service is similar to sites like YouTube, which offer revenue sharing to content creators.

Facebook declined to clarify just how it flagged Tsu for spam; why it blocked all links to Tsu.co instead of simply blocking the app; or why it aruges that Tsu is incentivizing sharing but YouTube isn t. Note, however, that YouTube removed the option to automatically post newly uploaded videos to Facebook in April.

Sobczak says he believes Facebook is blocking links to Tsu because it sees Tsu as a threat to its business model. Their model is based on taking other people s content, wrapping ads around it, he says. What s making Facebook worry, it s not that we re so big, it s the growth rate, and the philosophy that there s a better way to do things, a model where the content owners have complete ownership.

But the idea that Facebook feels threatened by Tsu seems unlikely. Facebook allows links from many other competitors, including Twitter, Tumblr, Pinterest and Ello. It also allows users to post links to social networks that promise to pay users to post, such as Bubblews. And the idea of sharing revenue with users is hardly a revolutionary. The model has been tried as far back as the mid-1990s by companies like the defunct Suite101, but it didn t stop the rise of sites like Wikipedia, LiveJournal and, eventually, Facebook, which invited users to post content for free. The idea of sharing wealth with users, however great it may be, is probably not keeping Mark Zuckerberg up at night.

In all likelihood, Tsu, Boing Boing and Tech News Today fell victim to an overzealous and under-supervised spam algorithm provoked by pyramid schemers. But the fact Facebook might not have knowingly acted to suppress a rival and unfavorable press coverage is of little comfort. Regardless of its reasons, the fact remains that Facebook did prevent people from sharing content that didn t violate its terms of service, including news stories and non-spam Tsu links posted manually.

Much has been made in recent month s of Facebook s increasing control over what we see online. The rise of social movements like Black Lives Matter are heavily dependent on social media, but Facebook s algorithms didn t initially surface many posts about the early days of the Ferguson, Missouri, protests last year. Publishers, meanwhile, depend upon Facebook to get their articles seen by their readers, and questions abound about what that s going to mean for the future of journalism. For example, what will happen if journalists use the company s Instant Articles program to publish pieces critical of Internet.org or the company s political lobbying or the Instant Articles program itself? Will publishers that aren t part of the Instant Articles program still be able to find an audience at all?

This power affects more than just journalists and activists. Facebook also is one of the primary platforms for getting word out about new apps, startups, and businesses of all types. To be banned from the platform could mean doom. That s an even bigger concern in developing countries where Facebook s Internet.org acts a sort of gatekeeper for the mobile internet. Although some have proposed regulating Google like a public utility, the Federal Communications Commission s new network neutrality regulations, which require Internet service providers to treat all traffic equally, will have no bearing on the likes of Google and Facebook, even as they amass more power to control what we see and do on the web.

Of course, all is not lost. Ferguson became an international news story despite Facebook s algorithmic apathy, largely in part through competitors like Twitter and Tumblr. Tsu will likely get more attention thanks to this snafu than it would have otherwise. If you can read this article, it means something is going right. But it could all go wrong in a hurry if we re not vigilant.

Google To Pull Chrome’s Patch Plug for 1-in-7 Windows and Mac Users

Google on Tuesday said it will switch off Chrome security updates in under five months for about one-in-seven Windows users and around the same portion of those running Apple’s OS X.

As of April 2016, Google will stop patching known Chrome vulnerabilities on 2001’s Windows XP and 2007’s Windows Vista. Together the two operating systems powered 14.8% of all Windows PCs last month.

The browser won’t suddenly refuse to work, but fixes for security flaws, including those that may already be in a hacker’s toolkit, will not be offered to Windows XP and Vista customers. Once April

arrives, users running those operating systems will not be served any Chrome updates, which often include not only bug fixes but also feature and functionality changes.

By dropping support for older editions of Windows and OS X, Chrome could lose about 14% of its user share if all those abandoned switched to another browser.

Google will also axe support for three older editions of OS X, the operating system exclusive to Apple's Macs: OS X Snow Leopard, Lion and Mountain Lion. The trio, also labeled as OS X 10.6, 10.7 and 10.8, respectively, were introduced in 2009, 2011 and 2012.

Last month, Snow Leopard, Lion and Mountain Lion accounted for 14.6% of all OS X editions whose users went online, according to Web analytics company Net Applications.

"Such older platforms are missing critical security updates and have a greater potential to be infected by viruses and malware," said Marc Pawliger, the director of engineering for Chrome, in a brief post on a Google blog. "If you are still on one of these unsupported platforms, we encourage you to move to a newer operating system to ensure that you continue to receive the latest Chrome versions and features."

With the exception of Windows Vista, all the operating systems facing the Chrome support guillotine have already been abandoned by their maker. Microsoft retired Windows XP, for instance, in April 2014, while Apple put Snow Leopard, Lion and Mountain Lion out to pasture in September of 2013, 2014 and 2015, respectively. Only Windows Vista continues to receive security updates from Microsoft; it won't get the heave-ho until April 2017.

Even Microsoft's and Apple's own browsers have been largely retired for their outdated OSes. Microsoft no longer patches bugs in Internet Explorer 8 (IE8) on Windows XP, although it still updates IE9 on Windows Vista. Apple last refreshed its Safari browser on Snow Leopard in May 2012, on Lion in August 2014, and on Mountain Lion in August 2015.

Beginning in April, Google will patch and upgrade the desktop version of Chrome only on Windows 7, Windows 8, Windows 8.1, Windows 10, OS X Mavericks, OS X Yosemite and OS X El Capitan.

Chrome's desertion of Windows XP was expected - in fact, Google had previously pegged the end of this year as the retirement timeline - but the abandonment of Vista and the three OS X editions had not been hinted at earlier.

Google likely believed purging the still-supported Vista was a no-brainer because of its low user share, a Net Applications estimate that serves as a proxy for the portion of the world's desktop and notebook personal computers that run a specific OS. In October, Vista's user share was just 2% of all Windows-equipped machines.

Mozilla's Firefox browser supports all the operating systems that Chrome will leave in the ditch, and so will become - assuming Mozilla doesn't mimic Google before April - the best option for

most of those left behind by Chrome.

Mozilla is typically the most cautious of the top four browser makers in pulling support. It didn't retire Firefox on Windows 2000, for example, until April 2012, more than a dozen years after its debut and nearly two years after Microsoft stopped updating the once-widely-used OS.

Chrome has been on a remarkable run since the beginning of 2015, accumulating 8.5 percentage points in user share since Jan. 1. That represented an increase of more than a third. In October, Chrome's user share stood at 31.1%, a record.

So while Google's decision to end support for the five operating systems next year may dampen growth as OS laggards move on to, say, Firefox, the impact will probably be minor because of Chrome's strong position. If the kill switch had been thrown now, not slated for April, Google's browser would face a maximum downturn of 4.5 percentage points if all Chrome users on Windows XP, Vista, and OS X Snow Leopard, Lion and Mountain Lion, suddenly deserted the browser. That's very unlikely: Those users are probably as indifferent to using an obsolete browser as they are to running an outdated OS.

Although a decline of that magnitude would be an embarrassing reverse for Google, it would not unseat Chrome from its second-place spot in the browser standings.

Lapsed Apple Certificate Triggers Massive Mac App Fiasco

A lapsed Apple digital certificate today triggered a massive app fiasco that prevented Mac users from running software they'd purchased from the Mac App Store.

"Whenever you download an app from the Mac App Store, the app provides a cryptographically-signed receipt," explained Paul Haddad, a co-founder of Tapbots, the company behind the popular Tweetbot Twitter client, in an email reply to questions today. "These receipts are signed with various certificates with different expiration dates. One of those is the 'Mac App Store Receipt Signing;' that expires every two years. That certificate expired on 'Nov 11 21:58:01 2015 GMT,' which caused most existing App Store receipts to no longer be considered valid."

Whoops.

The result: Bedlam.

Until Apple replaced the expired certificate, users who booted up their Macs today were unable to launch the apps they had bought through the Mac App Store, the OS X version of the iPhone's distribution portal.

But even after Apple replaced the outdated certificate, many apps still refused to run or threw off scary error messages, including one that said the app was "damaged and can't be opened," and others that said the app was already being used on another Mac,

when it was, in fact, not.

Some Computerworld staffers instead were asked to re-enter their Apple account credentials - those used to originally buy the apps - in a too-fleeting dialog, or were stymied when clicking on an app in the Dock simply did nothing and displayed no alert, warning or error message.

Most users were forced to delete the dysfunctional apps, then download and reinstall them from the Mac App Store to restore them to working order.

The problem impacted most if not all paid apps bought through the Mac App Store; the bulk of paid apps regularly check with Apple’s servers to make sure that a receipt exists for the purchase before running. "I’m guessing most paid Mac App Store apps will do this. Free ones may not bother," said Haddad, when explaining why some users haven’t been affected.

Haddad also said that some underlying problems remained in Apple’s e-store infrastructure. "Apple is now creating receipts which will expire in 2017, [but] for some reason some part of the Store infrastructure on [OS X] is either not requesting these new receipts until after a reboot or not properly validating them [emphasis added]. Either way, there’s still a bug somewhere in OS X."

As Haddad mentioned, the certificates Apple uses have a two-year lifespan. In fact, the problem cropped up two years ago and will likely reoccur in 2017.

Craig Hockenberry, a partner at the development firm IconFactory, pointed out a similar issue in October 2013, and filed a bug report with Apple.

In a Thursday tweet, Haddad noted that the new certificate will expire on Oct. 23, 2017. "Hopefully, Apple fixes whatever caching issues by then," he said.

Haddad’s advice for afflicted Mac users was to first reboot their machine, before going doing the delete-reinstall dance. "After a reboot OS X will grab a new receipt and that likely requires at least one log-in to your iTunes account," he said.

Apple did not immediately reply to questions about the snafu.

Ancillary Copyright 2.0: The European Commission Is Preparing A Frontal Attack on the Hyperlink

The European Commission is preparing a frontal attack on the hyperlink, the basic building block of the Internet as we know it. This is based on an absurd idea that just won t die: Making search engines and news portals pay media companies for promoting their freely accessible articles.

Earlier attempts at establishing this principle resulted in Germany s and Spain s ancillary copyright laws for press

publishers. These attempts backfired with tremendous collateral damage. In the European Parliament I was able to defeat repeated attempts by EPP MEPs to sneak into my copyright report text passages asking for an extension of these laws to the European level. But this newest attempt is the most dangerous yet.

According to a draft communication on copyright reform leaked yesterday (via IPKat), the Commission is considering putting the simple act of linking to content under copyright protection. This idea flies in the face of both existing interpretation and spirit of the law as well as common sense. Each weblink would become a legal landmine and would allow press publishers to hold every single actor on the Internet liable.

In the draft at hand, the Commission bemoans a lack of clarity about which actions on the Internet need a permission and which ones do not: in legal terms, they put forward the question when something is an act of communication to the public .

This is a reference to a ruling of the European Court of Justice in the Svensson case. While on one hand the judges established that the simple act of linking to publicly available content is no copyright infringement, because it does not reach a new public, a few questions were left open bis this ruling, however: For example when exactly content can be seen as accessible by the public and how e.g. links surpassing paywalls are to be treated.

The key point is that the Commission frames ancillary copyright laws for press publishers as an attempt by a few member states to solve this problem legally. Instead of criticizing the substance of these laws they only bemoan the possible fragmentation of European law by these different implementations. A coherent European answer to the problem behind all this is a neccessity. The reform of the executive rights on an EU-level is aparantly another attempt to fulfil the goals also pursued through the introduction of ancillary copyright law.

However, the depiction of this goal by the Commission is playinly wrong: Ancillary copyright laws do not answer the questions poised by the European Court of Justice. It is rather an attempt to cross-finance struggling publishing houses by asking thriving internet companies such as google to pay up for linking to publicly available articles to give price tags to exactly the same act of linking that has been clearly pronounced non-infringing by the European Court of Justice.

The Commission seems to want to reach the same by defining exclusive rights further, so the clarity it seeks can only mean: sheer linking to content protected by copyright shall be seen as providing access to them, and require therefore explicit permission. This plan is a departure from the basic principle behind the Svensson ruling, which permitted free linking on the Internet, without the need for active examination of whom the linked material belongs to.

Digital commissioner Günther Oettinger (CDU EPP), afiirmed dozens of times over the last months that he is considering the introduction of an instrument on the European level to compensate the publishing houses sinking income caused by lower sales and less income through advertisement:

Even Martin Schulz (SPD S&D), President of the European Parliament, struck a similair tone this week at the Publishers Summit when he confirmed that we need to clarify the relation between press publishers and digital platforms in the matter of copyright.

The publishers are clearly wielding so much influence through lobbying that there is nothing that can stop big-party politicians from trying to misapply copyright law in order to support obsolete business models:

Not the complete failure of pushed-through legislation like the one in Germany where not only the hoped-for increase in revenue stayed away, but where the fast and meek introduction of a free licence for google, a grand backpedalling by the publishing houses, is a possible violation of German law.

Not the collateral damage done to Spain s IT-economy, where the ancillary copyright law forbid granting free licences, making the collection of newspaper articles by non-profit organizations illegal even when publishers would like to support it; and forcing Google to completely shut off it s news service in Spain due to lack of profitability.

Not the vast majority of thousands of Europeans asking for the freedom of linking in the Commission s copyright consultation.

Not the exclamation of our IT-industry and warnings from scientists.

Not the repeated distinct rejection of introducing such plans into the report on the copyright directive by the European Parliament.

The prospective instrument Needing permission to link to something would be the bluntest tool yet employed for a completely mistaken cause that is being pushed through against all odds. This would have even more dramatic effects than everything seen so far regarding ancillary copyright laws in Germany and Spain.

Posting, sharing and sending links is a trivial every-day activity. It is impossible for both users and internet platforms to examine the legal status of every link. Content can change constantly online, so these examinations would actually have to take place constantly. What is more, every link leads to texts or pictures copyrighted by someone no matter whether they know it or not; no matter whether they want to profit from this or not.

Subsequently there will be legal uncertainty, confusion, and waves of dissuasion carrying legal fees for everybody it would sever the Internet s neurons in order to promote the interests of the few. We can not let that happen!

The leaked text is not a law proposal, but just a summary of the Commission s plans for next year. The plan is supposed to go public on the 9th of December. Affecting change in the now-known versions is nigh impossibly until then. But sometimes controversial proposals are leaked to test them if there is no protest, the plan can be unworriedly pursued.

It is hence even more important to become active now! Tell the Commission that pursuing the introduction of ancillary copyright

law means barking up the wrong tree no matter whether it is introduced as a privilege, or a restriciton to free linking is enacted. Do not allow the vested interests of the publishers lobby to destroy free communication on the Internet! Remind your representatives of them having rejected such approaches to introduce ancillary copyright laws with clear majorities in the past. Many representatives are worried about the competitiveness of European companies explain to them that liability for linking brings uncalculable risks with it for the European IT-industry and threatens to nip innovation in the bud! Encourage them to make clear once and for all:

Stop breaking the Internet!

Windows 10’s First Major Update Is Arriving Today

Microsoft has been testing a fresh update to Windows 10 for the past few months, and now it s ready to release it to everyone. More than 110 million machines are now running Windows 10, and they ll all be offered the update today. The update includes a number of fixes and UI changes that were originally planned for the final version of Windows 10.

One of the noticeable differences is a new colored title bar for desktop apps. All apps now feel a little more similar to the ones designed specifically for Windows 10, and Microsoft has also improved the context menus throughout the OS to make them a little bigger and darker to match the general theme. Another big change is the introduction of Skype integration with dedicated Messaging and Skype Video apps. They re both available from the Windows Store, and they re designed to offer basic access to messaging, audio, and video calls without having to download the full version of Skype.

Most other changes are fairly minor, including improved system icons. Microsoft is allowing Windows 10 users to now install apps to external storage, and some tablet mode improvements allow you to swipe down to close apps and snap apps more easily. Microsoft is also improving its Edge browser and Cortana in the Windows 10 Fall Update. Edge now syncs favorites, settings, and the reading list, alongside a new tab preview feature. Cortana will now work without a Microsoft Account, and the digital assistant can now understand inked notes in the Windows 10 Fall Update. The update is rolling out today from Windows Update.

Updates to Chrome Platform Support

Earlier this year, we announced that Google Chrome would continue support for Windows XP through the remainder of 2015. At that time, we strongly encouraged users on older, unsupported platforms such as Windows XP to update to a supported, secure operating

system. Such older platforms are missing critical security updates and have a greater potential to be infected by viruses and malware.

Today, we re announcing the end of Chrome s support for Windows XP, as well as Windows Vista, and Mac OS X 10.6, 10.7, and 10.8, since these platforms are no longer actively supported by Microsoft and Apple. Starting April 2016, Chrome will continue to function on these platforms but will no longer receive updates and security fixes.

If you are still on one of these unsupported platforms, we encourage you to move to a newer operating system to ensure that you continue to receive the latest Chrome versions and features.

=~=~=~=